AMENDMENTS TO THE CLAIMS

Listing of Claims

The following listing of claims replaces all previous versions.

1. (Currently Amended) A computer system providing Internet protocol security without secure domain name resolution, the system comprising:

a local domain name service (DNS) server that is communicatively coupled to a processor and that includes a secure Internet security protocol (IPSEC) cache, wherein the secure IPSEC cache is readable only by an Internet protocol (IP) processing layer of an operating system that controls execution of an application program by the processor, and wherein each cache entry comprises information that uniquely associates the cache entry with a particular application process or execution time;

a security policy data store that is communicatively coupled to the IP processing layer;

a computer-readable medium accessible to the processor and comprising one or more sequences of instructions which, when executed by the processor, cause the processor to carry out the steps of:

receiving a message generated as a result of execution of the application program and that contains a domain name;

receiving a data packet from the application;

in response to receiving the data packet from the application, searching the secure IPSEC cache for an entry that matches the domain name, wherein the searching comprises ~~verifying~~ using the information that uniquely associates the cache entry with a particular application process or execution time to verify that the domain name in the entry matches the domain name contained in the message;

querying the security policy data store for an IPSEC policy matching the domain name, wherein the IP processing layers verifies that the policy matches the domain name contained in the message;

in response to obtaining an IPSEC policy, applying the IPSEC policy to the data packet ~~message~~; and

purging the matching entry from the cache.

2. (Currently Amended) A computer system as recited in Claim 1, wherein the secure IPSEC cache comprises a plurality of cache entries, wherein each cache entry comprises a DNS name, one or more corresponding IP addresses~~, and information that uniquely associates the cache entry with a particular application process or execution time~~.

3. (Original) A computer system as recited in Claim 2, wherein the step of searching the secure IPSEC cache further comprises the step of searching the secure IPSEC cache for an entry that matches a process identifier of the application program, based on the information that uniquely associates the cache entry with a particular application process or execution time.

4. (Original) A computer system as recited in Claim 2, wherein the information that uniquely associates the cache entry with a particular application process or execution time comprises a process identifier value and a transaction identifier value.

5. (Original) A computer system as recited in Claim 4, wherein the step of searching the secure IPSEC cache further comprises the step of searching the secure IPSEC cache for an entry that matches a process and transaction associated with the application program, based on the process identifier value and transaction identifier value in the cache.

6. (Original) A computer system as recited in Claim 1, further comprising the step of querying the security policy database for an IPSEC policy based on an IP address that is resolved from the domain name received from the application program only when a matching cache entry is not found by searching the cache based on the domain name.

7. (Original) A computer system as recited in Claim 1, further comprising the steps of:

receiving a request to resolve a DNS name into network addresses;

resolving the DNS name using the local DNS server, resulting in generating one or more network addresses corresponding to the DNS name;

determining identifier information that uniquely associates the request with a particular application process or execution time; and

storing the DNS name, the network addresses, and the identifier information as an entry in the secure IPSEC cache.

8. (Currently Amended) A method for providing Internet protocol security without secure domain name resolution, the method comprising the computer-implemented steps of:

receiving a message generated as a result of execution of an application program and that contains a domain name;

receiving a data packet from the application;

in response to receiving the data packet from the application, searching a secure Internet security protocol (IPSEC) cache for an entry that matches the domain name, ~~wherein the searching comprises verifying the that domain name in the entry matches the domain name contained in the message,~~ wherein the secure IPSEC cache is communicatively coupled to a local domain name service (DNS) server, and wherein the secure IPSEC cache is readable only by an Internet protocol (IP) processing layer of an operating system that controls execution of the application program, and wherein each cache entry comprises information that uniquely associates the cache entry with a particular application process or execution time; and further wherein the searching comprises using the information that uniquely associates the cache entry with a particular application process or execution time to verify that the domain name in the entry matches the domain name contained in the message;

in response to obtaining an IPSEC policy, querying a security policy data store that is communicatively coupled to the IP processing layer for an IPSEC policy matching the domain name, wherein the IP processing layers verifies that the policy matches the domain name contained in the message;

applying the IPSEC policy to the data packet ~~message~~; and

purging the matching entry from the cache.

9. (Currently Amended) A method as recited in Claim 8, wherein the secure IPSEC cache comprises a plurality of cache entries, wherein each cache entry comprises a DNS name, one or more corresponding IP addresses~~, and information that uniquely associates the cache entry with a particular application process or execution time~~.

10. (Original) A method as recited in Claim 9, wherein the step of searching the secure IPSEC cache further comprises the step of searching the secure IPSEC cache for an entry that matches a process identifier of the application program, based on the information that uniquely associates the cache entry with a particular application process or execution time.

11. (Original) A method as recited in Claim 9, wherein the information that uniquely associates the cache entry with a particular application process or execution time comprises a process identifier value and a transaction identifier value.

12. (Original) A method as recited in Claim 11, wherein the step of searching the secure IPSEC cache further comprises the step of searching the secure IPSEC cache for an entry that matches a process and transaction associated with the application program, based on the process identifier value and transaction identifier value in the cache.

13. (Original) A method as recited in Claim 8, further comprising the step of querying the security policy database for an IPSEC policy based on an IP address that is resolved from the domain name received from the application program only when a matching cache entry is not found by searching the cache based on the domain name.

14. (Original) A method as recited in Claim 8, further comprising the steps of:
receiving a request to resolve a DNS name into network addresses;
resolving the DNS name using the local DNS server, resulting in generating one or more network addresses corresponding to the DNS name;
determining identifier information that uniquely associates the request with a particular application process or execution time; and
storing the DNS name, the network addresses, and the identifier information as an entry in the secure IPSEC cache.

15. (Previously Presented) A computer-readable medium carrying one or more sequences of instructions for providing Internet protocol security without secure domain name resolution, which instructions, when executed by one or more processors, cause the one or more processors to carry out the steps of:
receiving a message generated as a result of execution of an application program and that contains a domain name;
receiving a data packet from the application;
in response to receiving the data packet from the application, searching a secure Internet security protocol (IPSEC) cache for an entry that matches the domain name, ~~wherein the searching comprises verifying the that domain name in the entry matches the domain name contained in the message,~~ wherein the secure IPSEC cache is communicatively coupled to a local domain name service (DNS) server, and wherein the secure IPSEC cache is readable only by an Internet protocol (IP) processing layer of an operating system that controls execution of the application program, and wherein each cache entry comprises information that uniquely associates the cache entry with a particular application process or execution time; and further wherein the searching comprises using the information that uniquely associates the cache entry with a particular application process or execution time to verify that the domain name in the entry matches the domain name contained in the message;

in response to obtaining an IPSEC policy, querying a security policy data store that is communicatively coupled to the IP processing layer for an IPSEC policy matching the domain name, wherein the IP processing layers verifies that the policy matches the domain name contained in the message;

applying the IPSEC policy to the data packet ~~message~~; and

purging the matching entry from the cache.

16-21. (Canceled)

22. (Currently Amended) An apparatus for providing Internet protocol security without secure domain name resolution, comprising:

means for receiving a message generated as a result of execution of an application program and that contains a domain name;

means for receiving a data packet from the application;

means for searching a secure Internet security protocol (IPSEC) cache for an entry that matches the domain name, ~~wherein the searching comprises verifying the that domain name in the entry matches the domain name contained in the message,~~ wherein the secure IPSEC cache is communicatively coupled to a local domain name service (DNS) server, and wherein the secure IPSEC cache is readable only by an Internet protocol (IP) processing layer of an operating system that controls execution of the application program, and wherein each cache entry comprises information that uniquely associates the cache entry with a particular application process or execution time; and wherein the means for searching comprises means for using the information that uniquely associates the cache entry with a particular application process or execution time to verify that the domain name in the entry matches the domain name contained in the message;

means for querying a security policy data store that is communicatively coupled to the IP processing layer for an IPSEC policy matching the domain name, wherein the IP processing layers verifies that the policy matches the domain name contained in the message;

means for applying the IPSEC policy to the data packet ~~message~~; and

means for purging the matching entry from the cache.

23. (Currently Amended) An apparatus for providing Internet protocol security, without secure domain name resolution, for messages that are carried by a packet-switched data network, comprising:

a network interface that is coupled to the data network for receiving one or more packet flows therefrom;

a processor;

one or more stored sequences of instructions which, when executed by the processor, cause the processor to carry out the steps of:

receiving a message generated as a result of execution of an application program and that contains a domain name;

receiving a data packet from the application;

in response to receiving the data packet from the application, searching a secure Internet security protocol (IPSEC) cache for an entry that matches the domain name, ~~wherein the searching comprises verifying the that domain name in the entry matches the domain name contained in the message,~~ wherein the secure IPSEC cache is communicatively coupled to a local domain name service (DNS) server, and wherein the secure IPSEC cache is readable only by an Internet protocol (IP) processing layer of an operating system that controls execution of the application program, and wherein each cache entry comprises information that uniquely associates the cache entry with a particular application process or execution time; and further wherein the searching comprises using the information that uniquely associates the cache entry with a particular application process or execution time to verify that the domain name in the entry matches the domain name contained in the message;

in response to obtaining an IPSEC policy, querying a security policy data store that is communicatively coupled to the IP processing layer for an IPSEC policy matching the domain name, wherein the IP processing layers verifies that the policy matches the domain name contained in the message;

applying the IPSEC policy to the data packet ~~message~~; and

purging the matching entry from the cache.

24. (New) An apparatus as recited in Claim 22, wherein the secure IPSEC cache comprises a plurality of cache entries, wherein each cache entry comprises a DNS name, one or more corresponding IP addresses.

25. (New) A apparatus as recited in Claim 24, wherein the means for searching the secure IPSEC cache further comprises means for searching the secure IPSEC cache for an entry that matches a process identifier of the application program, based on the information that uniquely associates the cache entry with a particular application process or execution time.

26. (New) A apparatus as recited in Claim 25, wherein the information that uniquely associates the cache entry with a particular application process or execution time comprises a process identifier value and a transaction identifier value.

27. (New) A apparatus as recited in Claim 26, wherein the means for searching the secure IPSEC cache further comprises means for searching the secure IPSEC cache for an entry that matches a process and transaction associated with the application program, based on the process identifier value and transaction identifier value in the cache.

28. (New) A apparatus as recited in Claim 22, further comprising means for querying the security policy database for an IPSEC policy based on an IP address that is resolved from the domain name received from the application program only when a matching cache entry is not found by searching the cache based on the domain name.

29. (New) An apparatus as recited in Claim 22, further comprising:
means for receiving a request to resolve a DNS name into network addresses;
means for resolving the DNS name using the local DNS server, resulting in generating one or more network addresses corresponding to the DNS name;

means for determining identifier information that uniquely associates the request with a particular application process or execution time; and

means for storing the DNS name, the network addresses, and the identifier information as an entry in the secure IPSEC cache.